Abstract

The Electronic Voting (E-Voting) became a truly crucial part in the democracy of our life in which the election data is recorded, stored and prepared fundamentally as computerized data. Important basic properties of E-Voting are eligibility, privacy, fairness, uniqueness, receipt-freeness and verifiability. In addition to properties of blind signature such as correctness, blindness, anonymity and unforgeability. Blind signature allows to obtain a signature from the signer who signs a message without reading the content of the message. This paper presented a survey on blind signature schemes based on ElGamal Signature. The aim of this paper is to compare the existing blind signature schemes based on modifications of their parameters such as blinding factor, blinded message, blind signature, and Signature pair that satisfy these basic properties.
19. Mala, Hamid, and Nafiseh Nezhadansari, "New blind signature schemes based on the
(elliptic curve) discrete logarithm problem," in Computer and Knowledge Engineering (ICCKE),
2013 3th International conference on. IEEE, Isfahan, Iran, 2013.
20. Biswal, Biswa Bhusan, "A Novel Blind Signature Scheme Based On Discrete Logarithm
giving message recovery," in Proceedings of the 1st ACM conference on Computer and
communications security, 1993.
22. Nyberg, Kaisa, and Rainer A. Rueppel, "Message recovery for signature schemes based

Index Terms

Computer Science Information Sciences

Keywords

E-Voting, Blind signature, ElGamal signature, universally forgeable Attack